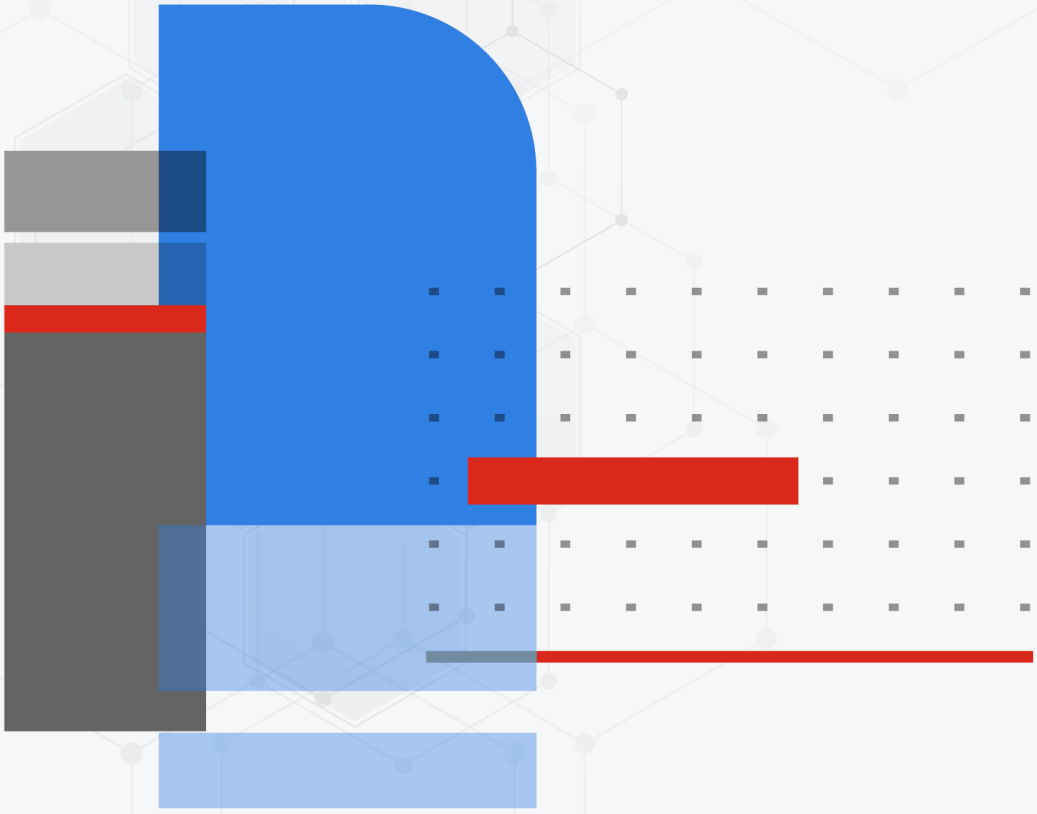
Release Notes

FortiAP-W2 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

Jun 8, 2023
FortiAP-W2 7.4.0 Release Notes
40-740-920460-20230608

TABLE OF CONTENTS

Change log

Date	Change description
2023-06-08	Initial release.

Introduction

This document provides release information for FortiAP-W2 version 7.4.0, build 0529:

For more information about your FortiAP device, see the *FortiWiFi and FortiAP Configuration Guide*.

Supported models

FortiAP-W2 version 7.4.0, build 0529 supports the following models:

Models
FAP-221E, FAP-222E, FAP-223E, FAP-224E, FAP-231E

FortiAP-W2 models do not have the unified threat management (UTM) functionality.

New features or enhancements

The following table includes FortiAP-W2 version 7.4.0 new features and enhancements:

Bug ID	Description

867684	Support WPA3-SAE security over the mesh backhaul.
	On the FortiGate CLI (FortiOS 7.4.0), add one mesh-backhaul vap with security wpa3-sae, and assign it to the mesh-root FortiAP.
	Note: The "Hash-to-Element (H2E) only" option is mandatory for the mesh backhaul.
	On the mesh-leaf FortiAP CLI, input the following mesh settings:
	`cfg -a MESH_AP_TYPE=1`
	`cfg -a MESH_AP_SSID=meshssidname`
	`cfg -a MESH_AP_SECURITY=2`
	`cfg -a MESH_AP_PASSWD=meshssidpassword`
	`cfg -c`

887980	Support a new data-channel security option "`ipsec-sn`". The FortiAP serial number is added to the initial IPsec setup message so that it can be used by a dispatcher to query the destination FortiGate. Then the FortiAP will connect to the FortiGate and encrypt the data channel with an IPsec-VPN tunnel.

Region/country code update and DFS certification

Bug ID	Description
916055	Enable DFS channels for FAP-221E Gen3 and FAP-223E Gen3 with region code "K".

Changes in CLI

Bug ID	Description
903756	A new `cfg` variable `MESH_AP_SECURITY` is added for the security mode of mesh-backhaul SSID. `cfg -a MESH_AP_SECURITY=0 | 1 | 2` Input 0 for "Open", 1 for "WPA/WPA2-Personal", or 2 for "WPA3-SAE". The default value is 0.

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.4.0

FortiAP-W2 version 7.4.0 supports upgrading from FortiAP-W2 version 7.2.2 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.4.0 supports downgrading to FortiAP-W2 version 7.2.2 and later.

Firmware image checksums

To get the MD5 checksum code for a Fortinet firmware image, perform the following steps:

1. Go to the Fortinet Support website.
2. Log in to your account. If you do not have an account, create one and then log in.
3. From the top banner, select **Download > Firmware Image Checksums**.
4. Enter the image file name, including the extension. For example, FAP_S221E-v600-build0233-FORTINET.out.
5. Click **Get Checksum Code**.

Supported upgrade paths

To view all previous FortiAP-W2 versions, build numbers, and their supported upgrade paths, see the Fortinet Documentation website.

Product integration and support

The following table lists product integration and support information for FortiAP-W2 version 7.4.0:

FortiOS	7.4.0 and later
Web browsers	Microsoft Edge version 41 and later
	Mozilla Firefox version 59 and later
	Google Chrome version 65 and later
	Apple Safari version 9.1 and later (for Mac OS X)
	Other web browsers may work correctly, but Fortinet does not support them.

We recommend that the FortiAP firmware version be matched with the respective FortiOS version, when available. Other variations of FortiOS and FortiAP versions may technically work for the lowest common feature set. However, if problems arise, Fortinet Support will ask that the versions be matched, as recommended, before troubleshooting.

Resolved issues

The following issues have been resolved in FortiAP-W2 version 7.4.0. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
371769	FortiAP could not suppress ARP poison attacks from wireless devices.
797151, 804661, 806019	Fixed various SNMP daemon crash issues.
878837	After the configuration of one SSID was changed, wireless clients on the other SSID got disconnected.
879756	Clients connected to one Leaf AP cannot communicate with clients connected to the other Leaf AP on the same Root AP.
883157	Wi-Fi clients would randomly get disconnected when FortiAP was sending statistics data to the FortiGate.
884413	Fixed a kernel panic issue `rgu_preempt self-detected stall on CPU`.
885589	Fixed a kernel panic issue `PC is at __kmalloc+0x114/0x1f0`.
885851	FortiAP with `AP_MGMT_VLAN_ID` configured would randomly get a connection loop after a firmware was provisioned from the FortiManager or FortiGate.
901128	Clients could not connect to the SSID on the 5GHz band as FortiAP would set the channel incorrectly after running for an extended period of time.

Known issues

The following issues have been identified in FortiAP-W2 version 7.4.0. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
537931	FAP-222E doesn't support the FortiAP Configuration mode. Push and hold the RESET button on the POE adapter for more than 5 seconds to reset FAP-222E to the factory default.
655887	FAP-221E/223E gets low throughput on tunnel SSID when its wtp-profile has set `dtls-policy ipsec-vpn`.
692160	Wireless packets captured by FortiAP radio in Sniffer mode are corrupted.

www.fortinet.com